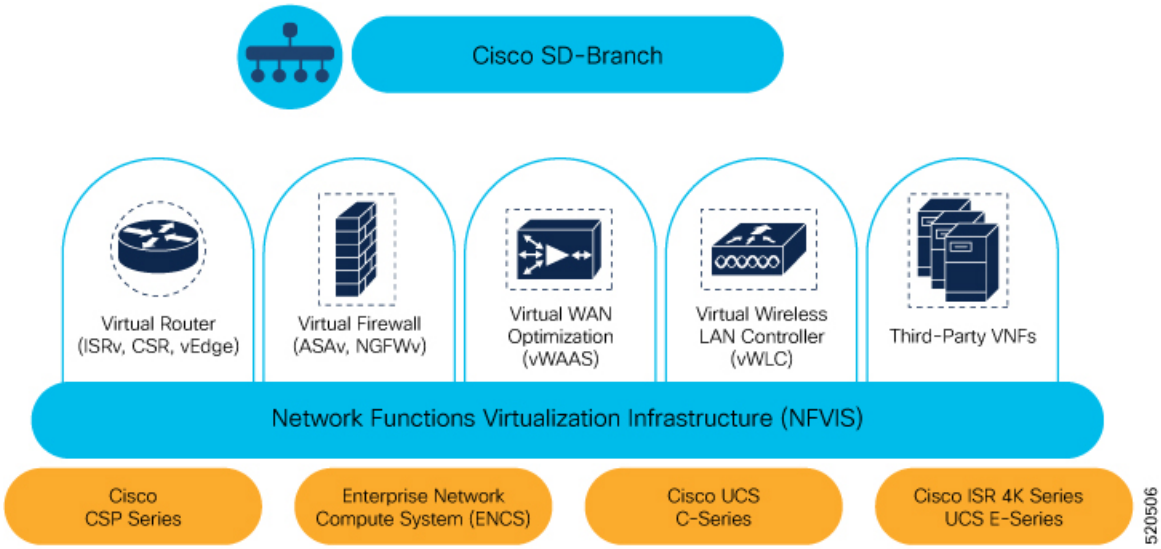
Define Cisco NFVIS SD-Branch Solution

Cisco SD-Branch solution is a full stack solution that delivers enterprise grade network and application services. You can choose from a variety of compute platforms that fits your design requirements. All the supported platforms has NFVIS as the host OS, for life cycle management of the SD-Branch device. The architecture allows zero touch provisioning of services in branch network compute devices using Cisco SD-WAN Manager.



Note NFVIS SD-Branch solution currently supports only ENCS 5400 devices.

- Create Authorized Device List, on page 1
- Create VNF Image Packages, on page 3
- Discover and Deploy Devices, on page 8

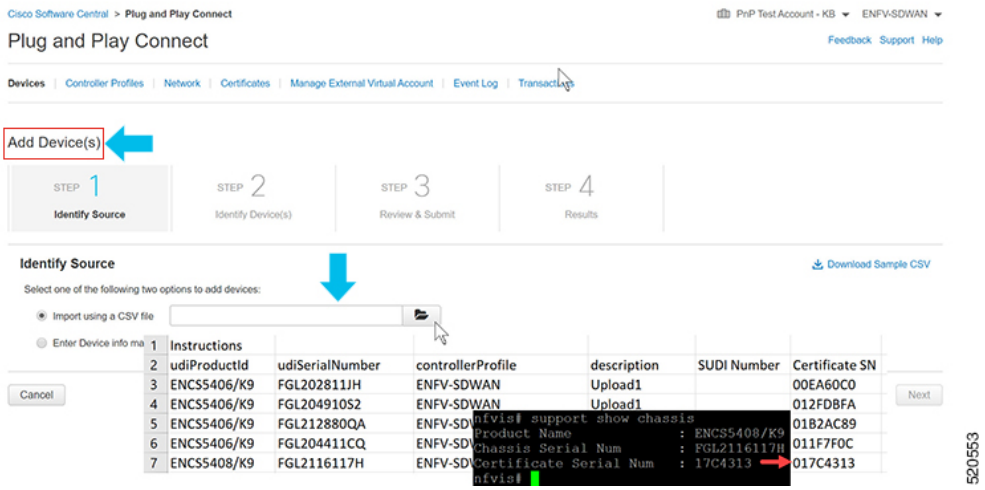
Create Authorized Device List

ENCS device serial numbers are uploaded into the customer specific Cisco Smart Account and virtual account. This is an automated process but, sometimes, you might have to manually create a virtual account and upload

ENCS device serial numbers. The following steps show you how to redirect a device at customer location to customer specific controller.

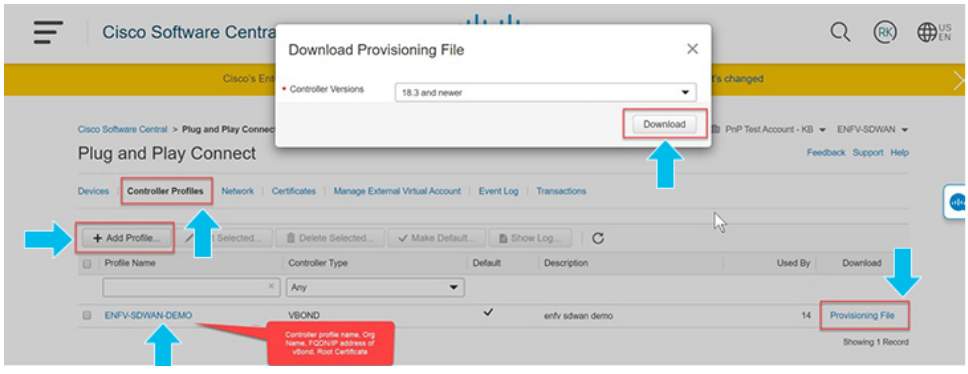
1. Add controller information to virtual account.

   - In PnP Connect server, select **Devices**, click **+ Add Devices** and upload a CSV file with information about PID, serial number and controller. You can upload a certificate issued by Symantec or upload enterprise root cert.



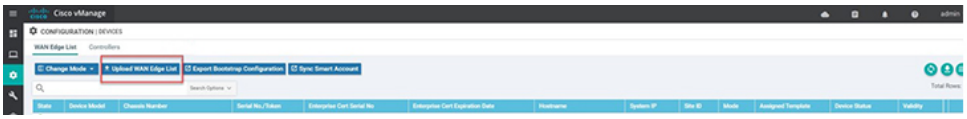
Note Starting from Cisco vManage 20.4, if the ENCS device certificate serial number is not available, the device serial number can be used to authenticate the device by populating the device serial number in the SUDI Number column. Cisco SD-WAN Manager smart sync uses the device serial number to authenticate the device.

   - Select **Controller Profiles** and click **+Add Profiles**. Enter details related to the controller to create a profile. Select **Provisioning File** and download it.



2. Add the device list to Cisco SD-WAN Manager.

   - Upload the authorized device list from virtual account to Cisco SD-WAN Manager.



Identity, Trust and Whitelist

Identity of the NFVIS WAN Edge device is uniquely identified by the chassis ID and certificate serial number. The following certificates are provided depending on the WAN Edge device:

- ENCS hardware device certificate is stored in the on-board SUDI chip installed during manufacturing. ENCS hardware is shipped with Cisco NFVIS software.
- Cisco Catalyst SD-WAN virtual devices do not have root certificates pre-installed on the device. For these devices, a One-Time Password (OTP) is provided by Cisco SD-WAN Manager to authenticate the device with the Cisco SD-WAN Control Components.

Trust of the WAN Edge devices is done using the root chain certificates that are pre-loaded in manufacturing, loaded manually, distributed automatically by Cisco SD-WAN Manager, or installed during Plug and Play (PnP) or Zero-Touch Provisioning (ZTP), the automated deployment provisioning process.

The Cisco SD-Branch solution uses a whitelist model, which means that the NFVIS WAN Edge devices that are allowed to join the SD-Branch overlay network need to be known by all the SD-Branch controllers before hand. This is done by adding the WAN Edge devices in the PnP connect portal. The added WAN Edge devices are attached to the Cisco SD-WAN Validator profile contained in the PnP portal (associated with the SD-Branch overlay organization-name) to create a provisioning file. This file is imported into the SD-Branch Cisco SD-WAN Control Components, which then automatically shares the device whitelist with the rest of SD-Branch controllers (Cisco SD-WAN Validator). The provisioning file containing the device whitelist can also be synced directly from the PnP connect portal to Cisco SD-WAN Manager through a secure SSL connection using REST APIs.

Note The Cisco SD-WAN Control Components such as Cisco SD-WAN Manager, Cisco SD-WAN Validator and Cisco SD-WAN Controller and WAN Edge devices, should all be configured with the same organization-name to join the same SD-Branch overlay network.

Create VNF Image Packages

Table 1: Feature History Table

Feature Name	Release Information	Description
Support for Uploading Different VNF Image Packages	NFVIS 4.6.1 Cisco vManage Release 20.6.1	This feature allows you to register a VNF image by uploading seperate VNF packages for image package, scaffold, and disk image.

Uploading a prepackaged Cisco VM image, tar.gz is supported on Cisco SD-WAN Manager. You can also package the VM image by providing a root disk image in any of the supported formats (qcow2). Use the linux

command-line NFVIS VM packaging tool, nfvpt.py to package the qcow2 or create a customized VM image for Cisco SD-WAN Manager.

Note

- Download the prepackaged Cisco VM image from the ISRv Software Download Page and the scaffold files for third party VMs from the Scaffold Files for Third Party VMs Software Download Page.
- Each VM type such as a firewall can have multiple VM images that are uploaded to Cisco SD-WAN Manager from same or different vendors being added to the catalog. Also, different versions that are based on the release of the same VM can be added to the catalog. However, ensure that the VM name is unique.
- When you upload a Cisco Catalyst 8000V Edge Software image to Cisco SD-WAN Manager, you might see a failure message that says **Image type missing in image properties file**. To add the missing image properties, extract the compressed tar.gz file, open the **image_properties.xml** file, add **`<imageType>virtualmachines</imageType>`** to the code and save the file.

The Cisco VM image format can be bundled as *.tar.gz and can include:

- Root disk images to boot the VM.
- Package manifest for checksum validation of the file listing in the package.
- Image properties file in XML format that lists the VM meta data.
- (Optional) Day-0 configuration, other files that are required to bootstrap the VM.
- System generated properties file in XML format that lists the VM system properties

The VM images can be hosted on both HTTP server local repository that Cisco SD-WAN Manager hosts or the remote server.

If the VM is in NFVIS supported VM package format such as, tar.gz, Cisco SD-WAN Manager performs all the processing and you can provide variable key and values during VNF provisioning.

Upload Different Image Types

Starting from NFVIS release 4.6.1, the process of image registration is decoupled from the process of uploading image properties. You can register the VNF image by uploading it in any supported image format. The following image formats are supported:

- Image package: .tar.gz file for the complete image package.
- Scaffold: .tar.gz file comprising of only the metadata (image properties and day 0 configuration files).
- Disk image: .qcow2 disk image.

To upload the image types:

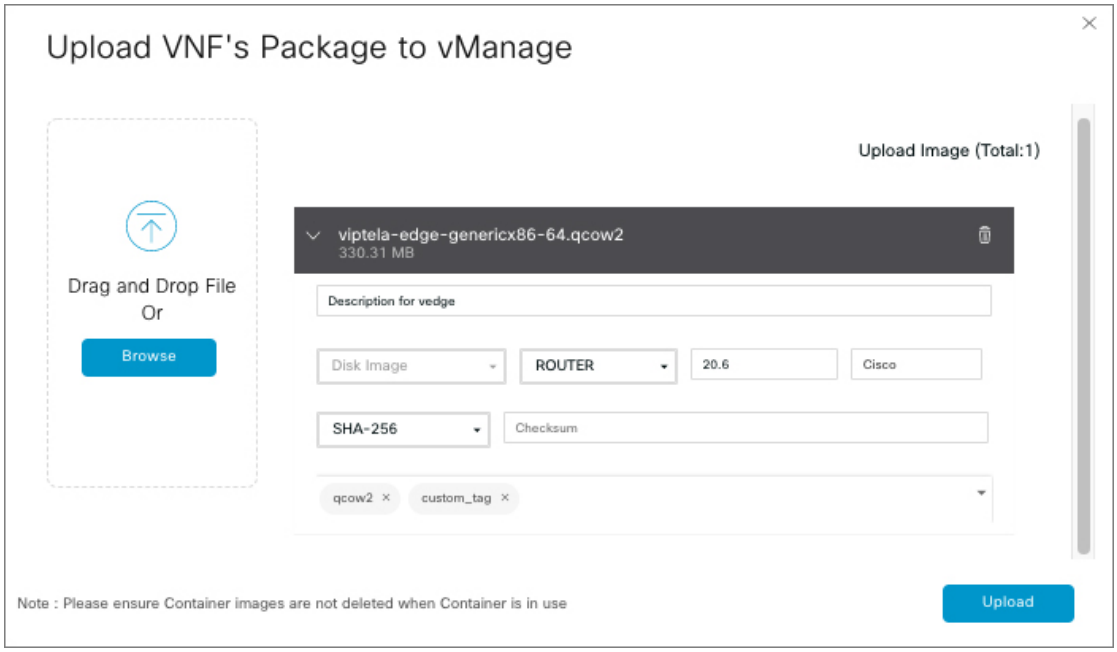
1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. From the **Upload Virtual Image** drop-down list, choose **vManage**.
4. In the **Upload VNF's Package to SD-WAN Manager** window upload your tar.gz or qcow2 file.

Note

- While uploading a Cisco Catalyst 8000V Edge Software image to Cisco SD-WAN Manager, you may encounter a failure message that says **Image type missing in image properties file**. To add the missing image properties, extract the compressed tar.gz file, open the **image_properties.xml** file, add **`<imageType>virtualmachines</imagetype>`** to the code and save the file.
- While uploading multiple VNF package files to Cisco SD-WAN Manager, you may encounter an error that states **failed to upload**. Uploading multiple VNF package files to Cisco SD-WAN Manager fails when the disk space allocated for the upload is less than 20% of the total partition size of the disk. Ensure to free up some disk space to upload multiple images.

5. From the **File Type** drop-down list, choose the image type (Image Package, Scaffold or Disk Image).
6. (Optional) Add descriptions and tags to help identify your image. You can either use the default tags available or create your own custom tags.
7. If you are uploading a disk image, choose values for **VNF Type**, **Version** and **Vendor**

   .

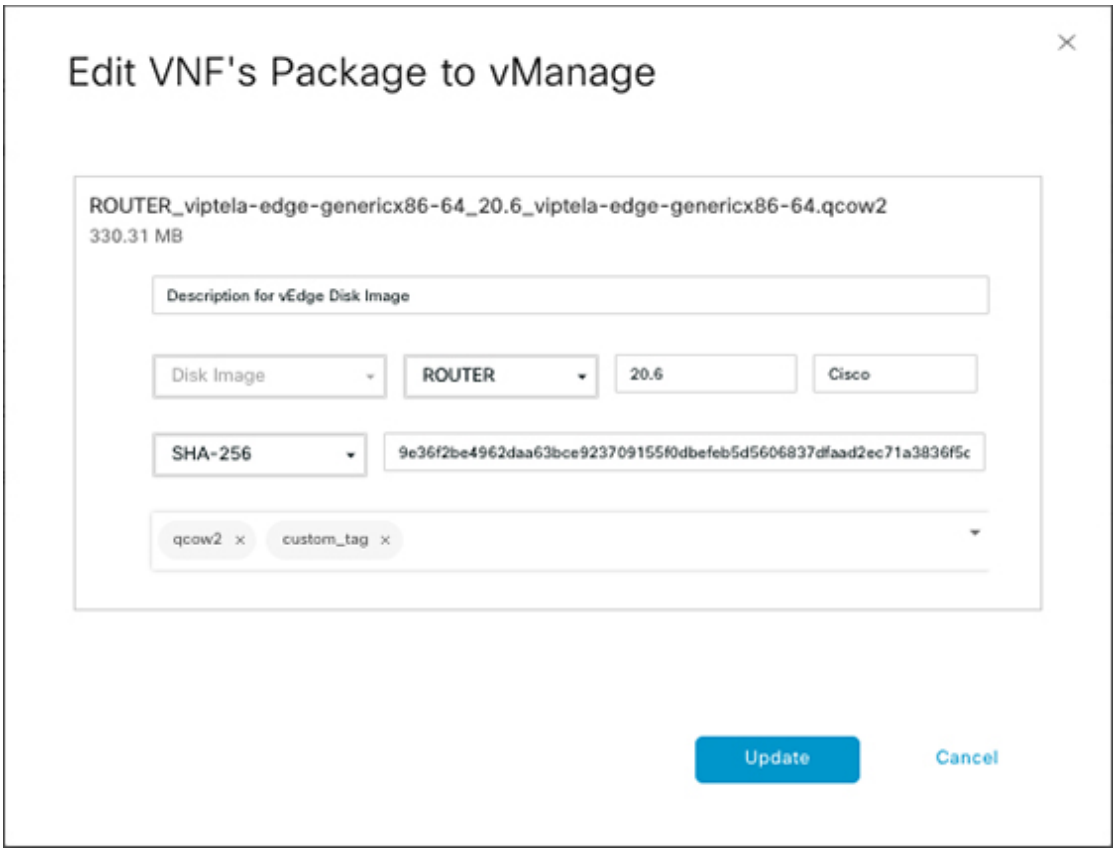


8. Click **Upload**

   .

To edit the VNF package:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. For the desired image, click **…** and choose **Edit**.



4. After making the desired changes, click **Update**.

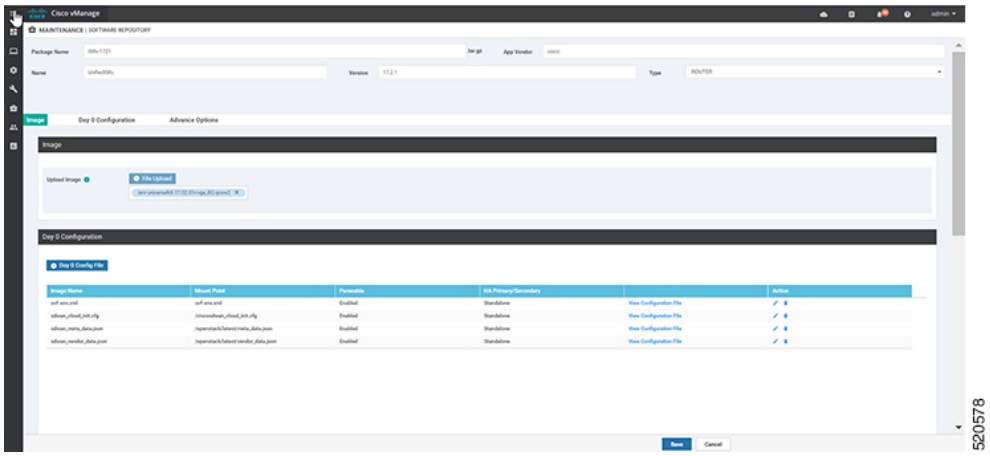
Note Cisco SD-WAN Manager only manages the Cisco VNFs, whereas Day-1 and Day-N configurations within VNF are not supported for other VNFs. See the NFVIS Configuration Guide, VM Image Packaging for more information about VM package format and content, and samples on image_properties.xml and manifest (package.mf).

To upload multiple packages for the same VM, same version, Communication Manager (CM) type, ensure that one of the three values (name, version, VNF type) are different. Then, you can repackage the VM *.tar.gz to be uploaded.

The following is an example of how to build an ISRv package:

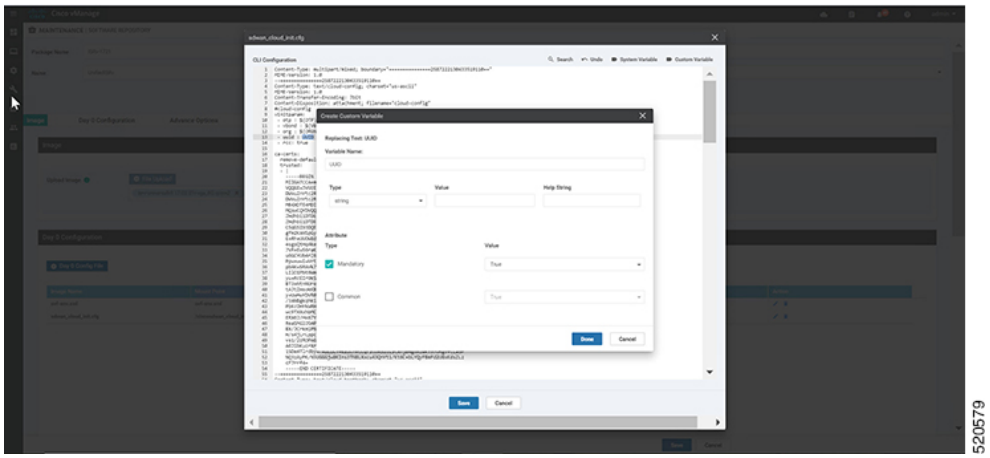
1. Upload the root disk image for bootstrap configurations.

   Click on **View Configuration File** next to the image.



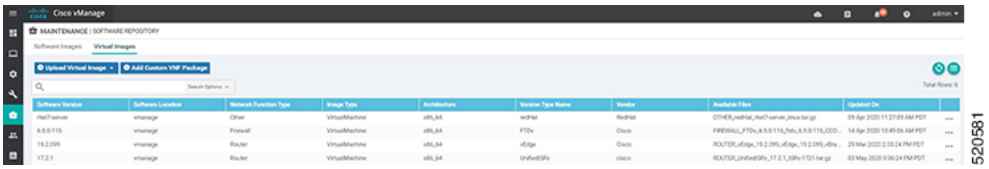
2. Select a variable and click on **Custom Variable**. In the pop-up window, select the variable type from the drop down menu.

   Click **Done** and then click **Save**.



3. You can select the image properties as per your requirements.

4. You can see the image package is created and added in the list of virtual images.



Discover and Deploy Devices

The WAN Edge device contacts the Cisco SD-WAN Validator on bootup, to establish a secure transient DTLS control connection. The Cisco SD-WAN Validator information can be configured manually through CLI on the WAN Edge device, using an IP address or resolvable domain-name FQDN, or it can be obtained automatically through the PnP or ZTP process.

The SD-Branch controllers (Cisco SD-WAN Validator, Cisco SD-WAN Manager and Cisco SD-WAN Controller) and WAN Edge devices need to mutually authenticate and trust each other before establishing the secure control connections. When the SD-Branch controllers authenticate each other and WAN Edge devices, they:

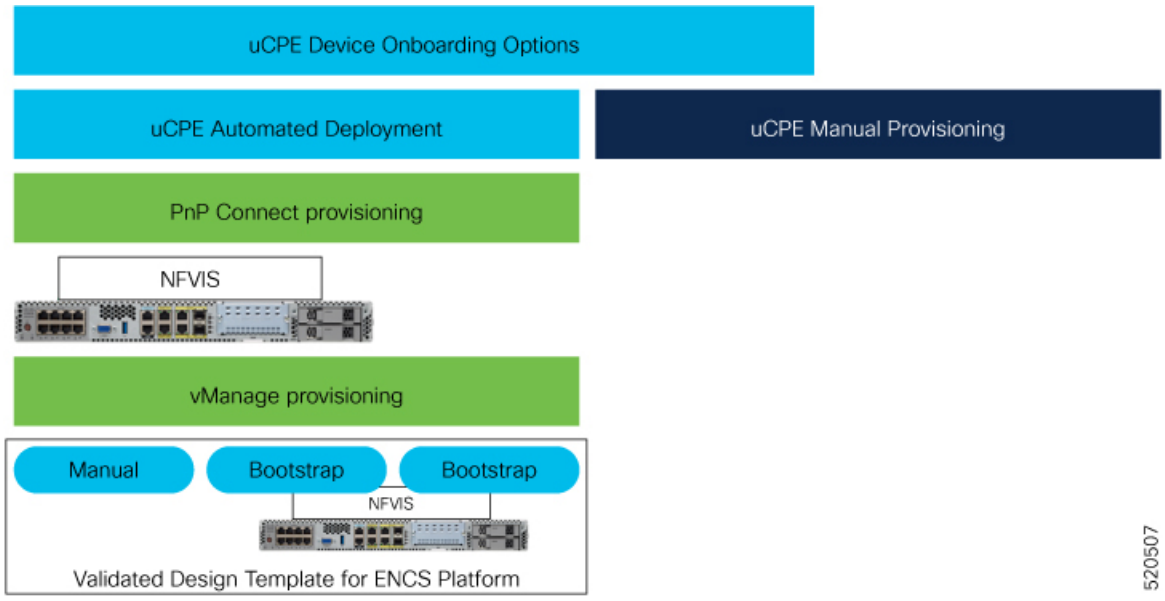
- Validate the root of trust for the certificate root CA
- Compare the organization-name of the received certificate Organization Unit (OU) against the locally configured
- Compare the certificate serial number against the authorized whitelist

When the WAN Edge devices authenticate the controllers, they:

- Validate the root of trust for the certificate root CA
- Compare the organization-name of the received certificate OU against the locally configured.

After successful authentication, the Cisco SD-WAN Validator establishes a secure transient DTLS control connection and then shares the Cisco SD-WAN Manager IP addresses. At this time, the Cisco SD-WAN Validator informs the other SD-branch controllers (Cisco SD-WAN Manager and Cisco SD-WAN Controller) to expect a control connection request from the WAN Edge device. ENCS device, unlike Cisco Catalyst SD-WAN devices does not maintain a control connection with Cisco SD-WAN Controller.

NFVIS WAN Edge device, upon learning the Cisco SD-WAN Manager information, initiates a control connection to the Cisco SD-WAN Manager server. After a successful authentication, a separate secure persistent DTLS/TLS connection is established. Cisco SD-WAN Manager provisions the configuration using the NETCONF protocol based on the device template attached to the WAN Edge device.



Default behavior of the NFVIS WAN Edge device is to establish:

- Secure transient DTLS control connection to Cisco SD-WAN Validator across one WAN transport, only during the onboarding process.
- Secure permanent DTLS/TLS control connection to Cisco SD-WAN Manager across a single WAN transport.